Конспект по Матлогу. Часть 1

Штукенберг Дмитрий

под редакцией Чепелина Вячеслава

Содержание

1 Лекция 5.

1.1 Введение в исчисление предикатов

<u>def:</u> Силлогизм — «подытоживание, подсчёт, умозаключение»

<u>def:</u> Категорический — потому, что речь идёт о категориях (в философском смысле).

Определяем некоторые стандартные мыслительные блоки, с которыми у образованной аудитории есть навык работы. Цель — сделать неформальный человеческий язык чуть более формальным. Где важно: научный трактат, диспут, для исключения ошибок в рассуждениях.

Язык рассуждений понимается единым, без разделения на язык исследователя и предметный.

Пример категорического силлогизма:

$$\frac{\text{Каждый человек смертен} \qquad \text{Сократ есть человек}}{\text{Сократ смертен}}$$

Категорический силллогизм соединяет три термина:

предикат (больший термин, P)
субъект (меньший термин, S)
средний термин (M).

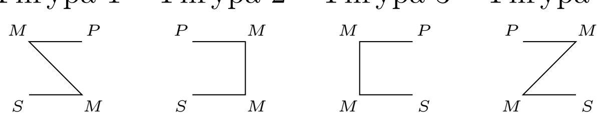
На основании соотношений P и M, а также M и S строим соотношение P и S.

Возможные соотношения:

A	Affirmato (общеутвердительное)	Матан есть раздел математики (SaP)
I	affIrmato (частноутвердительное)	Некоторые разделы математики сложны (SiP)
E	nEgo (общеотрицательное)	Никакой человек не знает всю математику
O	negO (частноотрицательное)	Некоторые разделы математики — не матан

<u>def:</u> Каждому силогизму соответствует **фигура**

Фигура 1 Фигура 2 Фигура 3 Фигура 4



	Фигура 1	Фигура 2	Фигура 3	Фигура 4
Большая посылка:	M—P	P—M	M—P	P—M
Меньшая посылка:	S—M	S—M	M—S	M—S
Заключение:	S—P	S—P	S—P	S—P

Расстановка соотношений вместо «—» в фигуре — модус. Например, тут — фигура 1, aaa.

$$\frac{\text{Каждый человек смертен} \qquad \text{Сократ есть человек}}{\text{Сократ смертен}}$$

Как этим пользоваться: по умозаключению (на русском языке) определяем, где в нём P, M, S и каковы между ними соотношения, находим соответствующую фигуру и модус, а дальше определяем силлогизм и его свойства в соответствии со следующими правилами.

Не все модусы осмысленны, большинство некорректно. Например фигура 1, aae:

$$\frac{\text{Каждый человек смертен} \qquad \text{Сократ есть человек}}{\text{Сократ не есть смертен}}$$

Список всех правильных модусов (из них выделяют *слабые*, выводящие частное соотношение при возможности общего — указаны курсивом):

Фигура 1	Фигура 2	Фигура 3	Фигура 4
Barbara	Cesare	Darapti	Bramantip
Celarent	Camestres	Disamis	Camenes
Darii	Festino	Datisi	Dimaris
Ferio	Baroco	Felapton	Fesapo
Barbari	*Cesaro*	Bocardo	Fresison
Celaront	*Camestros*	Ferison	*Camenos*

Некоторые модусы требуют непустоты M: это все слабые модусы и четыре сильных (указаны серым), например Darapti:

$$\frac{\text{Все единороги имеют рог} \qquad \text{Все единороги суть лошади}}{\text{Некоторые лошади имеют рог}}$$

Ограничения языка исчисления высказываний:

$$\frac{\text{Каждый человек смертен} \qquad \text{Сократ есть человек}}{\text{Сократ смертен}}$$

Цель: увеличить формализованную часть метаязыка.

Мы неформально знакомы с предикатами ($P : D \to V$) и кванторами ($\forall x.H(x) \to S(x)$).

$$\frac{\forall x.H(x) \to S(x) \qquad H(\text{Сократ})}{S(\text{Сократ})}$$

1.2 Язык исчисления предикатов

Пример:

$$\forall x.\sin x = 0 \lor (\sin x)^2 + 1 > 1$$

1. Предметные (здесь: числовые) выражения
   (a) Предметные переменные (x).
   (b) Одно- и двухместные функциональные символы «синус», «возведение в квадрат» и «сложение».
   (c) Нульместные функциональные символы «ноль» (0) и «один» (1).
2. Логические выражения
   (a) Предикатные символы «равно» и «больше»

1.2.1 Формальное определение

1. Два типа: предметные и логические выражения.
2. Предметные выражения: метапеременная θ.
   - Предметные переменные: a, b, c, ..., метапеременные x, y.
   - Функциональные выражения: $f(\theta_1, \dots, \theta_n)$, метапеременные f, g, ...
   - Примеры: r, $q(p(x, s), r)$.
3. Логические выражения: метапеременные α, β, γ, ...
   - Предикатные выражения: $P(\theta_1, \dots, \theta_n)$, метапеременная P. Имена: A, B, C, ...
   - Связки: $(\varphi \vee \psi)$, $(\varphi \mathbin{\&} \psi)$, $(\varphi \to \psi)$, $(\neg\varphi)$.
   - Кванторы: $(\forall x.\varphi)$ и $(\exists x.\varphi)$.

Сокращение записи и метаязык:

1. Метапеременные:
   - ψ, ϕ, π, ... — формулы
   - P, Q, ... — предикатные символы
   - θ, ... — термы
   - f, g, ... — функциональные символы
   - x, y, ... — предметные переменные
2. Скобки — как в И.В.; квантор — жадный:

$$(\forall a. \underbrace{A \vee B \vee C \to \exists b. \underbrace{D \mathbin{\&} \neg E}_{\exists b....}}_{\forall a....}) \mathbin{\&} F$$

3. Дополнительные обозначения при необходимости:
   - $(\theta_1 = \theta_2)$ вместо $E(\theta_1, \theta_2)$
   - $(\theta_1 + \theta_2)$ вместо $p(\theta_1, \theta_2)$
   - 0 вместо z
   - ...

1.3 Теория моделей исчисления предикатов

Напомним формулу:

$$\forall x. \sin x = 0 \vee (\sin x)^2 + 1 > 1$$

Без синтаксического сахара:

$$\forall x.E(s(x), z) \ \vee \ G(p(q(s(x)), o), o)$$

$$\forall x.E(s(x), z) \vee G(p(q(s(x)), o), o)$$

$$\forall x.E(s(x), z) \vee G(p(q(s(x)), o), o)$$

$$\forall x.E(s(x), z) \vee G(p(q(s(x)), o), o)$$

1. Истинностные (логические) значения:
   (a) предикаты (в том числе пропозициональные переменные = нульместные предикаты);
   (b) логические связки и кванторы.
2. Предметные значения:
   (a) предметные переменные;
   (b) функциональные символы (в том числе константы = нульместные функциональные символы)

1.3.1 Оценка исчисления предикатов

def: Оценка — упорядоченная четвёрка $\langle D, F, P, E\rangle$, где:

1. $D \neq \varnothing$ — предметное множество;
2. F — оценка для функциональных символов; пусть f_n — n-местный функциональный символ:
$$F_{f_n} : D^n \to D$$
3. P — оценка для предикатных символов; пусть T_n — n-местный предикатный символ:
$$P_{T_n} : D^n \to V \qquad V = \{\text{И}, \text{Л}\}$$
4. E — оценка для предметных переменных.
$$E(x) \in D$$

Запись и сокращения записи подобны исчислению высказываний:
$$[\![\phi]\!] \in V, \quad [\![Q(x, f(x)) \vee R]\!]^{x:=1, f(t):=t^2, R:=\text{И}} = \text{И}$$

1. Правила для связок $\vee$, $\&$, $\neg$, $\to$ остаются прежние;
2. $$[\![f_n(\theta_1, \theta_2, \ldots, \theta_n)]\!] = F_{f_n}([\![\theta_1]\!], [\![\theta_2]\!], \ldots, [\![\theta_n]\!])$$
3. $$[\![P_n(\theta_1, \theta_2, \ldots, \theta_n)]\!] = P_{T_n}([\![\theta_1]\!], [\![\theta_2]\!], \ldots, [\![\theta_n]\!])$$
4. $$[\![\forall x.\phi]\!] = \begin{cases} \text{И}, & \text{если } [\![\phi]\!]^{x:=t} = \text{И при всех } t \in D \\ \text{Л}, & \text{если найдётся } t \in D, \text{ что } [\![\phi]\!]^{x:=t} = \text{Л} \end{cases}$$
5. $$[\![\exists x.\phi]\!] = \begin{cases} \text{И}, & \text{если найдётся } t \in D, \text{ что } [\![\phi]\!]^{x:=t} = \text{И} \\ \text{Л}, & \text{если } [\![\phi]\!]^{x:=t} = \text{Л при всех } t \in D \end{cases}$$

Пример: Оценим:
$$[\![\forall a.\exists b.\neg a + 1 = b]\!]$$

1.3.2 Общезначимость и свободные переменные

def: Формула исчисления предикатов **общезначима**, если истинна при любой оценке:

$$\models \phi$$

То есть истинна при любых D, F, P и E.

Пример:

$$[\![\forall x.Q(f(x)) \vee \neg Q(f(x))]\!] = \text{И}$$

Доказательство:

Фиксируем D, F, P, E. Пусть $x \in D$. Обозначим $P_Q(F_f(E_x))$ за t. Ясно, что $t \in V$. Разберём случаи.

- Если $t = \text{И}$, то $[\![Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$, потому $[\![Q(f(x)) \vee \neg Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$
- Если $t = \text{Л}$, то $[\![\neg Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$, потому всё равно $[\![Q(f(x)) \vee \neg Q(f(x))]\!]^{Q(f(x)):=t} = \text{И}$

def: **Вхождение подформулы** в формулу — это позиция первого символа этой подформулы в формуле.

$$\text{Вхождения } x \text{ в формулу:} \quad (\forall x.A(x) \vee \exists x.B(x)) \vee C(x)$$

def: Рассмотрим формулу $\forall x.\psi$ (или $\exists x.\psi$). Здесь переменная x **связана** в ψ. Все вхождения переменной x в ψ — связанные.

def: Вхождение x в ψ **свободное**, если не находится в области действия никакого квантора по x. Переменная входит свободно в ψ, если имеет хотя бы одно свободное вхождение. $FV(\psi), FV(\Gamma)$ — множества свободных переменных в ψ, в Γ

Пример:

$$\psi[x := \theta] := \begin{cases} \psi, & \psi \equiv y, y \not\equiv x \\ \psi, & \psi \equiv \forall x.\pi \text{ или } \psi \equiv \exists x.\pi \\ \pi[x := \theta] \star \rho[x := \theta], & \psi \equiv \pi \star \rho \\ \theta, & \psi \equiv x \\ \forall y.\pi[x := \theta], & \psi \equiv \forall y.\pi \text{ и } y \not\equiv x \\ \exists y.\pi[x := \theta], & \psi \equiv \exists y.\pi \text{ и } y \not\equiv x \end{cases}$$

def: Терм θ **свободен для подстановки вместо** x в ψ ($\psi[x := \theta]$), если ни одно свободное вхождение переменных в θ не станет связанным после подстановки.

Свобода есть	Свободы нет
$(\forall x.P(y))[y := z]$	$(\forall x.P(y))[y := x]$
$(\forall y.\forall x.P(x))[x := y]$	$(\forall y.\forall x.P(t))[t := y]$

1.4 Теория доказательств исчисления предикатов

Рассмотрим язык исчисления предикатов. Возьмём все схемы аксиом классического исчисления высказываний и добавим ещё две схемы аксиом (здесь везде θ свободен для подстановки вместо x в φ):

11. $(\forall x.\varphi) \to \varphi[x := \theta]$
12. $\varphi[x := \theta] \to \exists x.\varphi$

Добавим ещё два правила вывода (здесь везде x не входит свободно в φ):

$$\frac{\varphi \to \psi}{\varphi \to \forall x.\psi} \text{ Правило для } \forall$$

$$\frac{\psi \to \varphi}{(\exists x.\psi) \to \varphi} \text{ Правило для } \exists$$

def: Доказуемость, выводимость, полнота, корректность — аналогично исчислению высказываний.

1.5 Теоремы о исчислении предикатов

1.5.1 Теорема о дедукции

Если $\Gamma \vdash \alpha \to \beta$, то $\Gamma, \alpha \vdash \beta$. Если $\Gamma, \alpha \vdash \beta$ и в доказательстве не применяются правила для кванторов по свободным переменным из α, то $\Gamma \vdash \alpha \to \beta$.

Доказательство:

$(\Rightarrow)$ — как в КИВ $(\Leftarrow)$ — та же схема, два новых случая.

Перестроим: $\delta_1, \delta_2, \ldots, \delta_n \equiv \beta$ в $\alpha \to \delta_1, \alpha \to \delta_2, \ldots, \alpha \to \delta_n$.

Дополним: обоснуем $\alpha \to \delta_n$, если предыдущие уже обоснованы.

Два новых похожих случая: правила для $\forall$ и $\exists$. Рассмотрим $\forall$.

Доказываем (n) $\alpha \to \psi \to \forall x.\varphi$ (правило для $\forall$), значит, доказано (k) $\alpha \to \psi \to \varphi$.

$(n-0.9)$	$(\alpha \to \psi \to \varphi) \to (\alpha \,\&\, \psi) \to \varphi$	Т. о полноте КИВ
$(n-0.6)$	$(\alpha \,\&\, \psi) \to \varphi$	М.Р. k,$n-0.8$
$(n-0.4)$	$(\alpha \,\&\, \psi) \to \forall x.\varphi$	Правило для $\forall$, $n-0.6$
$(n-0.3)$	$((\alpha \,\&\, \psi) \to \forall x.\varphi) \to (\alpha \to \psi \to \forall x.\varphi)$	Т. о полноте КИВ
(n)	$\alpha \to \psi \to \forall x.\varphi$	М.Р. $n-0.4$, $n-0.2$

Q.E.D.

def: $\gamma_1, \gamma_2, \ldots, \gamma_n \models \alpha$, если α выполнено всегда, когда выполнено $\gamma_1, \gamma_2, \ldots, \gamma_n$.

Теорема

Если $\Gamma \vdash \alpha$ и в доказательстве не используются кванторы по свободным переменным из Γ, то $\Gamma \models \alpha$

1.5.2 Корректность подстановки

Теорема.

Если θ свободен для подстановки вместо x в φ, то $[\![\varphi]\!]^{x:=[\![\theta]\!]} = [\![\varphi[x := \theta]]\!]$

Доказательство (индукция по структуре φ)

- База: φ не имеет кванторов. Очевидно.
- Переход: пусть справедливо для ψ. Покажем для $\varphi = \forall y.\psi$.
  - $x = y$ либо $x \notin FV(\psi)$. Тогда: $[\![\forall y.\psi]\!]^{x:=[\![\theta]\!]} = [\![\forall y.\psi]\!] = [\![(\forall y.\psi)[x := \theta]]\!]$
  - $x \neq y$. Тогда: $[\![\forall y.\psi]\!]^{x:=[\![\theta]\!]} = [\![\psi]\!]^{y\in D;x:=[\![\theta]\!]} = \dots$

    Свобода для подстановки: $y \notin \theta$.

    $$\dots = [\![\psi]\!]^{x:=[\![\theta]\!];y\in D} = \dots$$

    Индукционное предположение.

    $$\dots = [\![\psi[x := \theta]]\!]^{y\in D} = [\![\forall y.(\psi[x := \theta])]\!] = \dots$$

    Но $\forall y.(\psi[x := \theta]) \equiv (\forall y.\psi)[x := \theta]$ (как текст). Отсюда:

    $$\dots = [\![(\forall y.\psi)[x := \theta]]\!]$$

1.5.3 Корректность исчисления предикатов

Теорема. Если $\Gamma \vdash \alpha$ и в доказательстве не используются кванторы по свободным переменным из $FV(\Gamma)$, то $\Gamma \models \alpha$

Доказательство:

Фиксируем D, F, P. Индукция по длине доказательства α: при любом E выполнено $\Gamma \models \alpha$ при длине доказательства n, покажем для $n + 1$.

- Схемы аксиом (1)..(10), правило М.Р.: аналогично И.В.
- Схемы (11) и (12), например, схема $(\forall x.\varphi) \to \varphi[x := \theta]$:

$$[\![(\forall x.\varphi) \to \varphi[x := \theta]]\!] = [\![((\forall x.\varphi) \to \varphi)[x := \theta]]\!] = [\![(\forall x.\varphi) \to \varphi]\!]^{x:=[\![\theta]\!]} = \text{И}$$

- Правила для кванторов: например, введение $\forall$:

  Пусть $[\![\psi \to \varphi]\!] = \text{И}$. Причём $x \notin FV(\Gamma)$ и $x \notin FV(\psi)$. То есть, при любом $\S$ выполнено $[\![\psi \to \varphi]\!]^{x:=\S} = \text{И}$. Тогда $[\![\psi \to (\forall x.\varphi)]\!] = \text{И}$.

2 Лекция 6.

2.1 Теорема о полноте

Общая идея доказательства:

1. Надо справиться со слишком большим количеством вариантов. Модель задаётся как $\langle D, F, P, E\rangle$.
2. Для оценки в модели важно только какие формулы истинны. Поэтому факторизуем модели по истинности формул: модели $\mathcal{M}_1$ и $\mathcal{M}_2$ «похожи», если $[\![\varphi]\!]_{\mathcal{M}_1} = [\![\varphi]\!]_{\mathcal{M}_2}$ при всех φ.
3. Поступим так:
   (a) построим эталонное множество моделей $\mathfrak{M}$, каждая модель из него соответствует какому-то своему классу эквивалентности моделей;
   (b) докажем полноту $\mathfrak{M}$: если каждая $\mathcal{M} \in \mathfrak{M}$ предполагает $\mathcal{M} \models \varphi$, то $\vdash \varphi$;
   (c) заметим, что если $\models \varphi$, то каждая $\mathcal{M} \in \mathfrak{M}$ предполагает $\mathcal{M} \models \varphi$.
4. В ходе доказательства нас ждёт множество технических препятствий.

def: Γ — **непротиворечивое множество формул**, если $\Gamma \not\vdash \alpha \mathbin{\&} \neg\alpha$ для любого α

Примеры:

- непротиворечиво:
  - $\Gamma = \{A \to B \to A\}$
  - $\Gamma = \{P(x,y) \to \neg P(x,y), \forall x.\forall y.\neg P(x,y)\}$;
- противоречиво:
  - $\Gamma = \{P \to \neg P, \neg P \to P\}$

    так как $P \to \neg P, \neg P \to P \ \vdash \ \neg P \mathbin{\&} \neg\neg P$
- и ещё непротиворечиво: $\Gamma = \{P(1), P(2), P(3), \dots\}$

def: Γ — **полное непротиворечивое множество замкнутых бескванторных формул**, если:

1. Γ содержит только замкнутые бескванторные формулы;
2. если α — некоторая замкнутая бескванторная формула, то либо $\alpha \in \Gamma$, либо $\neg\alpha \in \Gamma$.

def: Γ — **полное непротиворечивое множество замкнутых формул**, если:

1. Γ содержит только замкнутые формулы;
2. если α — некоторая замкнутая формула, то либо $\alpha \in \Gamma$, либо $\neg\alpha \in \Gamma$.

Теорема:

Пусть Γ — непротивочивое множество замкнутых (бескванторных) формул. Тогда, какова бы ни была замкнутая (бескванторная) формула φ, хотя бы $\Gamma \cup \{\varphi\}$ или $\Gamma \cup \{\neg\varphi\}$ — непротиворечиво

Доказательство:

Пусть это не так и найдутся такие Γ, φ и α, что

$$\begin{aligned} \Gamma, \varphi &\vdash \alpha \mathbin{\&} \neg\alpha \\ \Gamma, \neg\varphi &\vdash \alpha \mathbin{\&} \neg\alpha \end{aligned}$$

Тогда по лемме об исключении гипотезы

$$\Gamma \vdash \alpha \mathbin{\&} \neg\alpha$$

То есть Γ не является непротиворечивым. Противоречие.

Q.E.D.

Теорема.

Пусть Γ — непротиворечивое множество замкнутых (бескванторных) формул. Тогда найдётся полное непротиворечивое множество замкнутых (бескванторных) формул Δ, что $\Gamma \subseteq \Delta$

Доказательство:

1. Занумеруем все формулы (их счётное количество): $\varphi_1, \varphi_2, \ldots$
2. Построим семейство множеств $\{\Gamma_i\}$:

   $$\Gamma_0 = \Gamma \quad \Gamma_{i+1} = \begin{cases} \Gamma_i \cup \{\varphi_i\}, & \text{если } \Gamma_i \cup \{\varphi_i\} \text{ непротиворечиво} \\ \Gamma_i \cup \{\neg\varphi_i\}, & \text{иначе} \end{cases}$$

3. Итоговое множество

   $$\Delta = \bigcup_i \Gamma_i$$

4. Непротиворечивость Δ не следует из индукции — индукция гарантирует непротиворечивость только Γ_i при натуральном (т.е. *конечном*) i, потому...

Q.E.D.

Завершение доказательства теоремы о полноте

Δ непротиворечиво:

1. Пусть Δ противоречиво, то есть

   $$\Delta \vdash \alpha \mathbin{\&} \neg\alpha$$

2. Доказательство конечной длины и использует конечное количество гипотез $\{\delta_1, \delta_2, \ldots, \delta_n\} \subset \Delta$, то есть

   $$\delta_1, \delta_2, \ldots, \delta_n \vdash \alpha \mathbin{\&} \neg\alpha$$

3. Пусть $\delta_i \in \Gamma_{d_i}$, тогда

   $$\Gamma_{d_1} \cup \Gamma_{d_2} \cup \cdots \cup \Gamma_{d_n} \vdash \alpha \mathbin{\&} \neg\alpha$$

4. Но $\Gamma_{d_1} \cup \Gamma_{d_2} \cup \cdots \cup \Gamma_{d_n} = \Gamma_{\max(d_1, d_2, \ldots, d_n)}$, которое непротиворечиво, и потому

   $$\Gamma_{d_1} \cup \Gamma_{d_2} \cup \cdots \cup \Gamma_{d_n} \nvdash \alpha \mathbin{\&} \neg\alpha$$

Q.E.D

2.2 Модели для множеств формул

def: **Моделью для множества формул** F назовём такую модель $\mathcal{M}$, что при всяком $\varphi \in F$ выполнено $[\![\varphi]\!]_{\mathcal{M}} = \text{И}$.

Альтернативное обозначение: $\mathcal{M} \models \varphi$.

Теорема.

Любое непротиворечивое множество замкнутых бескванторных формул имеет модель.

2.3 Конструкция модели

def: Пусть M — полное непротиворечивое множество замкнутых бескванторных формул. Тогда модель $\mathcal{M}$ задаётся так:

1. D — множество всевозможных предметных выражений без предметных переменных. Оно непусто (язык обычно содержит много нуль-местных функций), но если пусто — добавим туда какое-нибудь одно значение, пусть "z".
2. $[\![f(\theta_1, \dots, \theta_n)]\!] = \text{“f(”} + [\![\theta_1]\!] + \text{“,”} + \dots + \text{“,”} + [\![\theta_n]\!] + \text{“)”}$
3. $[\![P(\theta_1, \dots, \theta_n)]\!] = \begin{cases} \text{И}, & \text{если } P(\theta_1, \dots, \theta_n) \in M \\ \text{Л}, & \text{иначе} \end{cases}$
4. Так как $D \neq \varnothing$, то найдётся $z \in D$. Тогда $[\![x]\!] = z$. Это ничему не помешает, так как формулы замкнуты.

Лемма.

Пусть φ — бескванторная формула, тогда $\mathcal{M} \models \varphi$ тогда и только тогда, когда $\varphi \in M$.

Доказательство (индукция по длине формулы φ)

1. База. φ — предикат. Требуемое очевидно по определению $\mathcal{M}$.
2. Переход. Пусть $\varphi = \alpha \star \beta$ (или $\varphi = \neg\alpha$), причём $\mathcal{M} \models \alpha$ ($\mathcal{M} \models \beta$) тогда и только тогда, когда $\alpha \in M$ ($\beta \in M$).

   Тогда покажем требуемое для каждой связки в отдельности. А именно, для каждой связки покажем два утверждения:

   (a) если $\mathcal{M} \models \alpha \star \beta$, то $\alpha \star \beta \in M$.

   (b) если $\mathcal{M} \not\models \alpha \star \beta$, то $\alpha \star \beta \notin M$.

Q.E.D.

Если $\varphi = \alpha \to \beta$ и для любой формулы ζ, более короткой, чем φ, выполнено $\mathcal{M} \models \zeta$ тогда и только тогда, когда $\zeta \in M$, тогда:

1. если $\mathcal{M} \models \alpha \to \beta$, то $\alpha \to \beta \in M$;
2. если $\mathcal{M} \not\models \alpha \to \beta$, то $\alpha \to \beta \notin M$.

Доказательство (разбором случаев)

1. $\mathcal{M} \models \alpha \to \beta$: $[\![\alpha]\!] = \text{Л}$. Тогда по предположению $\alpha \notin M$, потому по полноте $\neg\alpha \in M$. И, поскольку в ИВ $\neg\alpha \vdash \alpha \to \beta$, то $M \vdash \alpha \to \beta$. Значит, $\alpha \to \beta \in M$, иначе по полноте $\neg(\alpha \to \beta) \in M$, что делает M противоречивым.

2. $\mathcal{M} \models \alpha \to \beta$: $[\![\alpha]\!] =$ И и $[\![\beta]\!] =$ И. Рассуждая аналогично, используя $\alpha, \beta \vdash \alpha \to \beta$, приходим к $\alpha \to \beta \in M$.
3. $\mathcal{M} \not\models \alpha \to \beta$. Тогда $[\![\alpha]\!] =$ И, $[\![\beta]\!] =$ Л, то есть $\alpha \in M$ и $\neg\beta \in M$. Также, $\alpha, \neg\beta \vdash \neg(\alpha \to \beta)$, отсюда $M \vdash \neg(\alpha \to \beta)$. Предположим, что $\alpha \to \beta \in M$, то $M \vdash \alpha \to \beta$ — отсюда $\alpha \to \beta \notin M$.

Завершение доказательства теоремы о существовании модели

Доказательство:

Пусть M — непротиворечивое множество замкнутых бескванторных формул.

По теореме о пополнении существует M' — полное непротиворечивое множество замкнутых бескванторных формул, что $M \subseteq M'$.

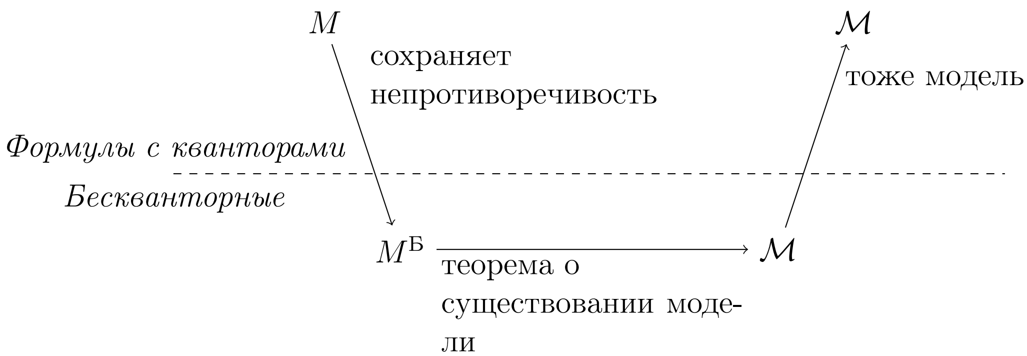
По лемме M' имеет модель, эта модель подойдёт для M.

2.4 Теорема Гёделя о полноте

Теорема Гёделя о полноте исчисления предикатов

Если M — непротиворечивое множество замкнутых формул, то оно имеет модель.

Схема доказательства



def: Формула φ имеет **поверхностные кванторы (находится в предварённой форме)**, если соответствует грамматике

$$\varphi ::= \forall x.\varphi \mid \exists x.\varphi \mid \tau$$

где τ — формула без кванторов

Теорема.

Для любой замкнутой формулы ψ найдётся такая формула φ с поверхностными кванторами, что $\vdash \psi \to \varphi$ и $\vdash \varphi \to \psi$

Индукция по структуре, применение теорем о перемещении кванторов.

Построение M^*

- Пусть M — полное непротиворечивое множество замкнутых формул с поверхностными кванторами (очевидно, счётное). Построим семейство непротиворечивых множеств замкнутых формул M_k.
- Пусть d_i^k — семейство *свежих* констант, в M не встречающихся.

- Индуктивно построим M_k:
  - База: $M_0 = M$
  - Переход: положим $M_{k+1} = M_k \cup S$, где множество S получается перебором всех формул $\varphi_i \in M_k$.
    1. φ_i — формула без кванторов, пропустим;
    2. $\varphi_i = \forall x.\psi$ — добавим к S все формулы вида $\psi[x := \theta]$, где θ — всевозможные замкнутые термы, использующие символы из M_k;
    3. $\varphi_i = \exists x.\psi$ — добавим к S формулу $\psi[x := d_i^{k+1}]$, где d_i^{k+1} — некоторая свежая, ранее не использовавшаяся в M_k, константа.

Лемма. Если M непротиворечиво, то каждое множество из M_k — непротиворечиво

Доказательство по индукции, база очевидна ($M_0 = M$). Переход:

- пусть M_k непротиворечиво, но M_{k+1} — противоречиво: $M_k, M_{k+1} \setminus M_k \vdash A \,\&\, \neg A$.
- Тогда (т.к. доказательство finite длины): $M_k, \gamma_1, \gamma_2, \dots, \gamma_n \vdash A \,\&\, \neg A$, где $\gamma_i \in M_{k+1} \setminus M_k$.
- По теореме о дедукции: $M_k \vdash \gamma_1 \to \gamma_2 \to \dots \to \gamma_n \to A \,\&\, \neg A$.
- Научимся выкидывать первую посылку: $M_k \vdash \gamma_2 \to \dots \to \gamma_n \to A \,\&\, \neg A$.
- И по индукции придём к противоречию: $M_k \vdash A \,\&\, \neg A$.

Q.E.D.

Лемма. Если $M_k \vdash \gamma \to W$ и $\gamma \in M_{k+1} \setminus M_k$, то $M_k \vdash W$.

Доказательство:

Покажем, как дополнить доказательство до $M_k \vdash W$, в зависимости от происхождения γ:

- Случай $\forall x.\varphi$: $\gamma = \varphi[x := \theta]$.

  Допишем в конец доказательства:

$\forall x.\varphi$	(гипотеза)
$(\forall x.\varphi) \to (\varphi[x := \theta])$	(сх. акс. 11)
γ	(M.P.)
W	(M.P.)

- Случай $\exists x.\varphi$: $\gamma = \varphi[x := d_i^{k+1}]$

  Перестроим доказательство $M_k \vdash \gamma \to W$: заменим во всём доказательстве d_i^{k+1} на y. Коллизий нет: под квантором d_i^{k+1} не стоит, переменной не является. Получим доказательство $M_k \vdash \gamma[d_i^{k+1} := y] \to W$ и дополним его:

$\varphi[x := y] \to W$	$\varphi[x := d_i^{k+1}][d_i^{k+1} := y]$
$(\exists y.\varphi[x := y]) \to W$	y не входит в W
$(\exists x.\varphi) \to (\exists y.\varphi[x := y])$	доказуемо (упражнение)
$\dots$	
$(\exists x.\varphi) \to W$	доказуемо как $(\alpha \to \beta) \to (\beta \to \gamma) \vdash \alpha \to \gamma$
$\exists x.\varphi$	гипотеза
W	

Q.E.D.

def: $M^* = \bigcup_k M_k$

Теорема M^* непротиворечиво.

Доказательство:

От противного: доказательство противоречия конечной длины, гипотезы лежат в максимальном M_k, тогда M_k противоречив.

def: $M^{\text{Б}}$ — множество всех бескванторных формул из M^*.

По непротиворечивому множеству M можем построить $M^{\text{Б}}$ и для него построить модель $\mathcal{M}$. Покажем, что эта модель годится для M^* (и для M, так как $M \subset M^*$).

Лемма. $\mathcal{M}$ есть модель для M^*.

Доказательство Покажем, что при $\varphi \in M^*$ выполнено $\mathcal{M} \models \varphi$. Докажем индукцией по количеству кванторов в φ.

- База: φ без кванторов. Тогда $\varphi \in M^{\text{Б}}$, отсюда $\mathcal{M} \models \varphi$ по построению $\mathcal{M}$.
- Переход: пусть утверждение выполнено для всех формул с n кванторами. Покажем, что это выполнено и для $n+1$ кванторов.
  - Рассмотрим $\varphi = \exists x.\psi$, случай квантор всеобщности — аналогично.
  - Раз $\exists x.\psi \in M^*$, то существует k, что $\exists x.\psi \in M_k$.
  - Значит, $\psi[x := d_i^{k+1}] \in M_{k+1}$.
  - По индукционному предположению, $\mathcal{M} \models \psi[x := d_i^{k+1}]$ — в формуле n кванторов.
  - Но тогда $[\![\psi]\!]^{x:=[\![d_i^{k+1}]\!]} = \text{И}$.
  - Отсюда $\mathcal{M} \models \exists x.\psi$.

Q.E.D.

Формулировка и доказательство теоремы Гёделя

Теорема Гёделя о полноте исчисления предикатов

Если M — замкнутое непротиворечивое множество формул, то оно имеет модель.

Доказательство:

- Построим по M множество формул с поверхностными кванторами M'.
- По M' построим непротиворечивое множество замкнутых бескванторных формул $M^{\text{Б}}$ ($M^{\text{Б}} \subseteq M^*$, теорема о непротиворечивости M^*).
- Дополним его до полного, построим для него модель $\mathcal{M}$ (теорема о существовании модели).
- $\mathcal{M}$ будет моделью и для M' ($M' \subseteq M^*$, лемма о модели для M^*), и, очевидно, для M.

2.5 Полнота исчисления предикатов

<u>**Следствие из теоремы Гёделя о полноте**</u> Исчисление предикатов полно.

Доказательство:

- Пусть это не так, и существует формула φ, что $\models \varphi$, но $\not\vdash \varphi$.
- Тогда рассмотрим $M = \{\neg\varphi\}$.
- M непротиворечиво: если $\neg\varphi \vdash A \,\&\, \neg A$, то $\vdash \varphi$ (упражнение).
- Значит, у M есть модель $\mathcal{M}$, и $\mathcal{M} \models \neg\varphi$.
- Значит, $[\![\neg\varphi]\!] =$ И, поэтому $[\![\varphi]\!] =$ Л, поэтому $\not\models \varphi$. Противоречие.

2.6 Непротиворечивость исчисления предикатов

<u>**Теорема.**</u> Если у множества формул M есть модель $\mathcal{M}$, оно непротиворечиво.

Доказательство:

Пусть противоречиво: $M \vdash A\&\neg A$, в доказательстве использованы гипотезы $\delta_1, \delta_2, \dots, \delta_n$. Тогда $\vdash \delta_1 \to \delta_2 \to \dots \to \delta_n \to A \,\&\, \neg A$, то есть $[\![\delta_1 \to \delta_2 \to \dots \to \delta_n \to A \,\&\, \neg A]\!] =$ И (корректность). Поскольку все $[\![\delta_i]\!]_{\mathcal{M}} =$ И, то и $[\![A \,\&\, \neg A]\!]_{\mathcal{M}} =$ И (анализ таблицы истинности импликации). Однако $[\![A \,\&\, \neg A]\!] =$ Л. Противоречие.

Следствие: Исчисление предикатов непротиворечиво

Доказательство:

Рассмотрим $M = \varnothing$ и любую классическую модель.

Доказательства опираются на непротиворечивость метатеории.

Q.E.D.

2.7 Теорема Гёделя о компактности

Если Γ — некоторое семейство бескванторных формул, то Γ имеет модель тогда и только тогда, когда любое его конечное подмножество имеет модель.

Доказательство:

($\Rightarrow$): очевидно

($\Leftarrow$): пусть каждое конечное подмножество имеет модель. Тогда Γ непротиворечиво:

Иначе для любой σ выполнено $\Gamma \vdash \sigma$. В частности, для $\gamma \in \Gamma$ выполнено $\Gamma \vdash \neg\gamma$. Доказательство имеет конечную длину и использует конечное количество формул $\gamma_1, \dots, \gamma_n \in \Gamma$. Тогда рассмотрим $\Sigma = \{\gamma, \gamma_1, \dots, \gamma_n\}$ и модель $\mathcal{S}$ для неё. Тогда:

1. $\models_S \gamma$ (определение модели)
2. $\models_S \neg\gamma$ (теорема о корректности: $\Sigma \vdash \neg\gamma$, значит $\Sigma \models \neg\gamma$ в любой модели)

Значит, Γ имеет модель (вспомогательная теорема к теореме Гёделя о полноте).

Q.E.D.

3 Лекция 7:

3.1 Машина Тьюринга

def: Машина Тьюринга:

1. Внешний алфавит $q_1, \ldots, q_n$, выделенный символ-заполнитель q_ε
2. Внутренний алфавит (состояний) $s_1, \ldots, s_k$; s_s — начальное, s_f — допускающее, s_r — отвергающее.
3. Таблица переходов $\langle k, s\rangle \Rightarrow \langle k', s', \leftrightarrow\rangle$

def: Состояние машины Тьюринга:

1. Бесконечная лента с символом-заполнителем q_ε, текст конечной длины.
2. Головка над определённым символом.
3. Символ состояния (состояние в узком смысле) — символ внутреннего алфавита.

Машина, меняющая все 0 на 1, а все 1 — на 0.

1. Внешний алфавит $\varepsilon, 0, 1$.
2. Внутренний алфавит s_s, s_f (начальное и допускающее состояния соответственно).
3. Переходы:

	ε	0	1
s_s	$\langle s_f, \varepsilon, \cdot\rangle$	$\langle s_s, 1, \rightarrow\rangle$	$\langle s_s, 0, \rightarrow\rangle$
s_f	$\langle s_f, \varepsilon, \cdot\rangle$	$\langle s_f, 0, \cdot\rangle$	$\langle s_f, 1, \cdot\rangle$

def: **Язык** — множество строк

def: Язык L **разрешим**, если существует машина Тьюринга, которая для любого слова w переходит в допускающее состояние, если $w \in L$, и в отвергающее, если $w \notin L$.

3.1.1 Неразрешимость задачи останова

def: Рассмотрим все возможные описания машин Тьюринга. Составим упорядоченные пары: описание машины Тьюринга и входная строка. Из них выделим язык останавливающихся на данном входе машин Тьюринга.

Теорема

Язык всех останавливающихся машин Тьюринга неразрешим

Доказательство:

От противного. Пусть $S(x, y)$ — машина Тьюринга, определяющая, остановится ли машина x, примененная к строке y.

W(x) = if (S(x,x)) { while (true); return 0; } else { return 1; }

Что вернёт $S(code(W), code(W))$?

Q.E.D.

Кодируем состояния:

1. внешний алфавит: n 0-местных функциональных символов $q_1, \ldots, q_n$; q_ε — символ-заполнитель.

2. список: ε и $c(l, s)$; «abc» представим как $c(q_a, c(q_b, c(q_c, \varepsilon)))$.
3. положение головки: «$ab\underline{p}q$» как $(c(q_b, c(q_a, \varepsilon)), c(q_p, c(q_q, \varepsilon)))$.
4. внутренний алфавит: k 0-местных функциональных символов $s_1, \dots, s_k$. Из них выделенные s_s — начальное и s_f — допускающее состояние.

Достижимые состояния:

Предикатный символ $F_{x,y}(w_l, w_r, s)$: если у машины x с начальной строкой y состояние s достижимо на строке $rev(w_l)@w_r$.

Будем накладывать условия: семейство формул C_m.

Очевидно, начальное состояние достижимо:

$$C_0 := F_{x,y}(\varepsilon, y, s_s)$$

Кодируем переходы:

1. Занумеруем переходы.
2. Закодируем переход m:

$$\langle k, s\rangle \Rightarrow \langle k', s', \rightarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

   $C_m = \forall w_l.\forall w_r.F_{x,y}(w_l, c(q_k, w_r), s_s) \rightarrow F_{x,y}(c(q_{k'}, w_l), w_r, s_{s'})$
   (здесь требуется, чтобы под головкой находился непустой символ q_k, потому мы обязательно требуем, чтобы лента была непуста)
3. Переход посложнее:

$$\langle k, s\rangle \Rightarrow \langle k', s', \leftarrow\rangle, \text{ в случае } q_k \neq q_\varepsilon$$

   $C_m = \forall w_l.\forall w_r.\forall t.F_{x,y}(c(t, w_l), c(q_k, w_r), s_s) \rightarrow F_{x,y}(w_l, c(t, c(q_{k'}, w_r)), s_{s'}) \& \forall w_l.\forall w_r.F_{x,y}(\varepsilon, c(q_k, w_r), s_s) \rightarrow F_{x,y}(\varepsilon, c(q_\varepsilon, c(q_{k'}, w_r)), s_{s'})$
4. и т.п.

Итоговая формула:

$$C = C_0 \,\&\, C_1 \,\&\, \cdots \,\&\, C_n$$

«правильное начальное состояние и правильные переходы между состояниями»

Теорема:

Состояние s со строкой $rev(w_l)@w_r$ достижимо тогда и только тогда, когда $C \vdash F_{x,y}(w_l, w_r, s)$

Доказательство:

($\Leftarrow$) Рассмотрим модель: предикат $F_{x,y}(w_l, w_r, s)$ положим истинным, если состояние достижимо. Это — модель для C (по построению C_m). Значит, доказуемость влечёт истинность (по корректности).

($\Rightarrow$) Индукция по длине лога исполнения.

Неразрешимость исчисления предикатов: доказательство

Теорема. Язык всех доказуемых формул исчисления предикатов неразрешим

Т.е. нет машины Тьюринга, которая бы по любой формуле α определяла, доказуема ли она.

Доказательство:

Пусть существует машина Тьюринга, разрешающая любую формулу. На её основе тогда несложно построить некоторую машину Тьюринга, перестраивающую любую машину S (с допускающим состоянием s_f и входом y) в её ограничения C и разрешающую формулу ИП $C \to \exists w_l . \exists w_r . F_{S,y}(w_l, w_r, s_f)$. Эта машина разрешит задачу останова.

Q.E.D.

3.2 Аксиоматика Пеано и формальная арифметика

«Бог создал целые числа, всё остальное — дело рук человека.»
Леопольд Кронекер, 1886 г.

1. Рациональные ($\mathbb{Q}$).

   $Q = \mathbb{Z} \times \mathbb{N}$ — множество всех простых дробей.

   $\langle p, q \rangle$ — то же, что $\frac{p}{q}$

   $\langle p_1, q_1 \rangle \equiv \langle p_2, q_2 \rangle$, если $p_1 q_2 = p_2 q_1$

   $\mathbb{Q} = Q/_{\equiv}$

2. Вещественные ($\mathbb{R}$). $X = \{A, B\}$, где $A, B \subseteq \mathbb{Q}$ — дедекиндово сечение, если:

   (a) $A \cup B = \mathbb{Q}$

   (b) Если $a \in A$, $x \in \mathbb{Q}$ и $x \leq a$, то $x \in A$

   (c) Если $b \in B$, $x \in \mathbb{Q}$ и $b \leq x$, то $x \in B$

   (d) A не содержит наибольшего.

   $\mathbb{R}$ — множество всех возможных дедекиндовых сечений.

   $\sqrt{2} = \{\{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}, \{x \in \mathbb{Q} \mid x > 0 \,\&\, x^2 > 2\}\}$

Целые числа тоже попробуем определить

$$\mathbb{Z} : \dots - 3, -2, -1, 0, 1, 2, 3, \dots$$

- $Z = \{\langle x, y \rangle \mid x, y \in \mathbb{N}_0\}$
- Интуиция: $\langle x, y \rangle = x - y$
- $$\begin{aligned} \langle a, b \rangle + \langle c, d \rangle &= \langle a + c, b + d \rangle \\ \langle a, b \rangle - \langle c, d \rangle &= \langle a + d, b + c \rangle \end{aligned}$$
- Пусть $\langle a, b \rangle \equiv \langle c, d \rangle$, если $a + d = b + c$. Тогда $\mathbb{Z} = Z/_{\equiv}$
- $0 = [\langle 0, 0 \rangle],\ 1 = [\langle 1, 0 \rangle],\ -7 = [\langle 0, 7 \rangle]$

3.3 Натуральные числа: аксиоматика Пеано

$$\mathbb{N} : 1, 2, \ldots \text{ или } \mathbb{N}_0 : 0, 1, 2, \ldots$$

def: N (или, более точно, $\langle N, 0, (')\rangle$) *соответствует* **аксиоматике Пеано**, если следующее определено/выполнено:

1. Операция «штрих» $(') : N \to N$, причём нет $a, b \in N$, что $a \neq b$, но $a' = b'$.

   Если $x = y'$, то x назовём следующим за y, а y — предшествующим x.
2. Константа $0 \in N$: нет $x \in N$, что $x' = 0$.
3. Индукция. Каково бы ни было свойство («предикат») $P : N \to V$, если:
   (a) $P(0)$
   (b) При любом $x \in N$ из $P(x)$ следует $P(x')$

   то при любом $x \in N$ выполнено $P(x)$.

Как построить? Например, в стиле алгебры Линденбаума:

1. N — язык, порождённый грамматикой $\nu ::= \texttt{0} \mid \nu\texttt{«'»}$
2. 0 — это «0», x' — это $x +$ «'»

3.3.1 Обозначения и определения

def: $1 = 0'$, $2 = 0''$, $3 = 0'''$, $4 = 0''''$, $5 = 0'''''$, $6 = 0''''''$, $7 = 0'''''''$, $8 = 0''''''''$, $9 = 0'''''''''$

def:

$$a + b = \begin{cases} a, & \text{если } b = 0 \\ (a + c)', & \text{если } b = c' \end{cases}$$

Например,

$$2 + 2 = 0'' + 0'' = (0'' + 0')' = ((0'' + 0)')' = ((0'')')' = 0'''' = 4$$

def:

$$a \cdot b = \begin{cases} 0, & \text{если } b = 0 \\ a \cdot c + a, & \text{если } b = c' \end{cases}$$

3.4 Уточнение исчисления предикатов

- Пусть требуется доказывать утверждения про равенство. Введём $E(p, q)$ — предикат «равенство».
- Однако $\nvdash E(p, q) \to E(q, p)$: если $D = \{0, 1\}$ и $E(p, q) ::= (p > q)$, то $\not\models E(p, q) \to E(q, p)$.
- Конечно, можем указывать $\forall p.\forall q.E(p, q) \to E(q, p) \vdash \varphi$.
- Но лучше добавим аксиому $\forall p.\forall q.E(p, q) \to E(q, p)$.
- Добавив необходимые аксиомы, получим *теорию первого порядка.*

3.5 Теория первого порядка

def: **Теорией первого порядка** назовём исчисление предикатов с дополнительными («нелогическими» или «математическими»):

- предикатными и функциональными символами;
- аксиомами.

Сущности, взятые из исходного исчисления предикатов, назовём *логическими*

3.6 Порядок логики/теории

Порядок	Кванторы	Формализует суждения...	Пример
нулевой	запрещены	об отдельных значениях	И.В.
первый	по предметным переменным	о множествах	И.П.
	$\{2, 3, 5, 7, \dots\} = \{t \mid \forall p.\forall q.(p \neq 1 \,\&\, q \neq 1) \to (t \neq p \cdot q)\}$		
второй	по предикатным переменным	о множествах множеств	Типы
	$S = \{\{t \mid P(t)\} \mid \varphi[p := P]\}$		
	...		

Пример логики 2 порядка

$\alpha \to \beta \to \alpha$ (сх. акс. 1)	$\forall a.\forall b.a \to b \to a$
`let rec map f l = match l with`	$map : \forall a.\forall b.(a \to b) \to a$ `list` $\to b$ `list`

```
| [] -> []
| l1::ls -> f l1 :: map f ls
map ((+) 1) [1;2;3] = [2;3;4]
```

3.7 Формальная арифметика

def: Формальная арифметика — теория первого порядка, со следующими добавленными нелогическими ...

- двухместными функциональными символами $(+)$, $(\cdot)$; одноместным функциональным символом $(')$, нульместным функциональным символом 0;
- двухместным предикатным символом $(=)$;
- восемью нелогическими *аксиомами*:

(A1) $a = b \to a = c \to b = c$	(A5) $a + 0 = a$
(A2) $a = b \to a' = b'$	(A6) $a + b' = (a + b)'$
(A3) $a' = b' \to a = b$	(A7) $a \cdot 0 = 0$
(A4) $\neg a' = 0$	(A8) $a \cdot b' = a \cdot b + a$

- нелогической схемой аксиом индукции $\psi[x := 0] \,\&\, (\forall x.\psi \to \psi[x := x']) \to \psi$ с метапеременными x и ψ.

Пример: Докажем, что $a = a$:

Пусть $\top ::= 0 = 0 \to 0 = 0 \to 0 = 0$, тогда:

(1)	$a = b \to a = c \to b = c$	(Акс. A1)
(2)	$(a = b \to a = c \to b = c) \to \top \to (a = b \to a = c \to b = c)$	(Сх. акс. 1)
(3)	$\top \to (a = b \to a = c \to b = c)$	(M.P. 1, 2)
(4)	$\top \to (\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(5)	$\top \to (\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(6)	$\top \to (\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(Введ. $\forall$)
(7)	$\top$	(Сх. акс 1)
(8)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c)$	(M.P. 7, 6)
(9)	$(\forall a.\forall b.\forall c.a = b \to a = c \to b = c) \to$ $\to (\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c)$	(Сх. акс. 11)
(10)	$\forall b.\forall c.a + 0 = b \to a + 0 = c \to b = c$	(M.P. 8, 9)
(12)	$\forall c.a + 0 = a \to a + 0 = c \to a = c$	(M.P. 10, 11)
(14)	$a + 0 = a \to a + 0 = a \to a = a$	(M.P. 12, 13)
(15)	$a + 0 = a$	(Акс. A5)
(16)	$a + 0 = a \to a = a$	(M.P. 15, 14)
(17)	$a = a$	(M.P. 15, 16)

4 Лекция 8.

4.1 Арифметизация в работах Лейбница

- Любой термин — пара взаимно простых чисел $+a - b$. Например, мудрый — $+70 - 33$, благочестивый — $+10 - 3$.
- Общеутвердительное предложение (каждый $+a - b$ есть $+c - d$): $a : c$ и $b : d$.
  Всякий мудрый есть благочестивый ($70 = 10 \cdot 7$, $33 = 3 \cdot 11$).
- Частноотрицательное предложение — не верно общеутвердительное.
- Общеотрицательное предложение — когда a, d или b, c имеют общий делитель, отличный от 1:
  Ни один благочестивый ($+10-3$) не есть несчастный ($+5-14$), так как $10 = 2 \cdot 5$ и $14 = 2 \cdot 7$.

4.2 Соглашения о записи

- Рассматриваем функции $\mathbb{N}_0^n \to \mathbb{N}_0$.
- Обозначим вектор $\langle x_1, x_2, \ldots, x_n \rangle$ как $\overrightarrow{x}$.

Примитивы Z, N, U, S

1. Примитив «Ноль» (Z)
$$Z : \mathbb{N}_0 \to \mathbb{N}_0, \qquad Z(x_1) = 0$$
2. Примитив «Инкремент» (N)
$$N : \mathbb{N}_0 \to \mathbb{N}_0, \qquad N(x_1) = x_1 + 1$$
3. Примитив «Проекция» (U) — семейство функций; пусть $k, n \in \mathbb{N}_0, k \le n$
$$U_n^k : \mathbb{N}_0^n \to \mathbb{N}_0, \qquad U_n^k(\overrightarrow{x}) = x_k$$
4. Примитив «Подстановка» (S) — семейство функций; пусть $g : \mathbb{N}_0^k \to \mathbb{N}_0, \quad f_1, \ldots, f_k : \mathbb{N}_0^n \to \mathbb{N}_0$
$$S\langle g, f_1, f_2, \ldots, f_k \rangle(\overrightarrow{x}) = g(f_1(\overrightarrow{x}), \ldots, f_k(\overrightarrow{x}))$$

Примитив «примитивная рекурсия», R

Пусть $f : \mathbb{N}_0^n \to \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$. Тогда $R\langle f, g \rangle : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$, причём

$$R\langle f, g\rangle(\overrightarrow{x}, y) = \begin{cases} f(\overrightarrow{x}), & y = 0 \\ g(\overrightarrow{x}, y-1, R\langle f, g\rangle(\overrightarrow{x}, y-1)), & y > 0 \end{cases}$$

$$\begin{aligned} R\langle f, g\rangle(\overrightarrow{x}, 3) &= g(\overrightarrow{x}, 2, R\langle f, g\rangle(\overrightarrow{x}, 2)) \\ &= g(\overrightarrow{x}, 2, g(\overrightarrow{x}, 1, R\langle f, g\rangle(\overrightarrow{x}, 1))) \\ &= g(\overrightarrow{x}, 2, g(\overrightarrow{x}, 1, g(\overrightarrow{x}, 0, R\langle f, g\rangle(\overrightarrow{x}, 0)))) \\ &= g(\overrightarrow{x}, 2, g(\overrightarrow{x}, 1, g(\overrightarrow{x}, 0, f(\overrightarrow{x})))) \end{aligned}$$

def: Функция f — **примитивно-рекурсивна**, если может быть выражена как композиция примитивов Z, N, U, S и R.

4.3 Примитивно-рекурсивные функции: $x + y$

Лемма: $f(a,b) = a + b$ примитивно-рекурсивна

Доказательство:

$f = R\langle U_1^1, S\langle N, U_3^3\rangle\rangle$:

$R\langle f, g\rangle(x,y) = \begin{cases} f(x), & y = 0 \\ g(x, y-1, R\langle f, g\rangle(x, y-1)), & y > 0 \end{cases}$

- База. $R\langle U_1^1, S\langle N, U_3^3\rangle\rangle(x, 0) = U_1^1(x) = x$
- Переход. $R\langle U_1^1, S\langle N, U_3^3\rangle\rangle(x, y+1) =$

  $... = S\langle N, U_3^3\rangle(x, y, R\langle U_1^1(x), S\langle N, U_3^3\rangle\rangle(x, y)) =$

  $... = S\langle N, U_3^3\rangle(x, y, x + y) =$

  $... = N(x + y) = x + y + 1$

Q.E.D.

Какие функции примитивно-рекурсивные?

1. Сложение, вычитание
2. Умножение, деление
3. Вычисление простых чисел
4. Неформально: все функции, вычисляемые конечным числом вложенных циклов `for`:

```
for (int i1 = 0; i1 < g1(x1...xn); i1++) {
    for (int i2 = 0; i2 < g2(x1...xn,i1); i2++) {
        ...
           for (int ik = 0; ik < gk(x1...xn,i1,i2...); ik++) {
               // выражение без циклов
           }
        ...
    }
}
```

4.4 Общерекурсивные функции

def: Функция — **общерекурсивная**, если может быть построена при помощи примитивов Z, N, U, S, R и примитива минимизации:

$$M\langle f\rangle(x_1, x_2, \ldots, x_n) = \min\{y : f(x_1, x_2, \ldots, x_n, y) = 0\}$$

Если $f(x_1, x_2, \ldots, x_n, y) > 0$ при любом y, результат не определён.

Пример: Пусть $f(x,y) = x - y^2$, тогда $\lceil\sqrt{x}\rceil = M\langle f\rangle(x)$

```
int sqrt(int x) {
    int y = 0;
    while (x-y*y > 0) y++;
    return y;
}
```

def: Функция Аккермана:

$$A(m,n) = \begin{cases} n+1, & m = 0 \\ A(m-1,1), & m > 0, n = 0 \\ A(m-1, A(m, n-1)), & m > 0, n > 0 \end{cases}$$

Теорема.

Пусть $f(\overrightarrow{x})$ — примитивно-рекурсивная. Тогда найдётся k, что $f(\overrightarrow{x}) < A(k, \max(\overrightarrow{x}))$

Доказательство:

Индукция по структуре f.

1. $f = Z$, тогда $k = 0$, т.к. $A(0, x) = x + 1 > Z(x) = 0$;
2. $f = N$, тогда $k = 1$, т.к. $A(1, x) = x + 2 > N(x) = x + 1$;
3. $f = U_s^n$, тогда $k = 0$, т.к. $f(\overrightarrow{x}) \leq \max(\overrightarrow{x}) < A(0, \max(\overrightarrow{x}))$;
4. $f = S\langle g, h_1, \ldots, h_n\rangle$, тогда $k = k_g + \max(k_{h_1}, \ldots, k_{h_n}) + 2$;
5. $f = R\langle g, h\rangle$, тогда $k = \max(k_g, k_h) + 2$.

Q.E.D.

Лемма: Пусть $f = R\langle g, h\rangle$. Тогда при $k = \max(k_g, k_h) + 2$ выполнено $f(\overrightarrow{x}, y) \leq A^{(y+1)}(k - 2, \max(\overrightarrow{x}, y))$.

Доказательство:

Индукция по y.

- База: $y = 0$. Тогда: $f(\overrightarrow{x}, 0) = g(\overrightarrow{x}) \leq A(k_g, \max(\overrightarrow{x})) \leq A^{(1)}(k-2, \max(\overrightarrow{x}, 0))$.
- Переход: пусть $f(\overrightarrow{x}, y) \leq A^{(y+1)}(k-2, \max(\overrightarrow{x}, y))$. Тогда $f(\overrightarrow{x}, y+1) = h(\overrightarrow{x}, y, f(\overrightarrow{x}, y)) \leq A(k_h, \max(\overrightarrow{x}, y, f(\overrightarrow{x}, y))) \leq A(k_h, \max(\overrightarrow{x}, y, A^{(y+1)}(k-2, \max(\overrightarrow{x}, y))) = A(k_h, A^{(y+1)}(k-2, \max(\overrightarrow{x}, y))) \leq A^{(y+2)}(k-2, \max(\overrightarrow{x}, y+1))$

Q.E.D.

Заметим, что $A^{(y+1)}(k-2, \max(\overrightarrow{x}, y)) \leq A^{(\max(\overrightarrow{x}, y)+1)}(k-2, \max(\overrightarrow{x}, y)) \leq A^{(\max(\overrightarrow{x}, y)+2)}(k-2, \max(\overrightarrow{x}, y)) < A(k, \max(\overrightarrow{x}, y))$

4.5 Тезис Чёрча

Тезис Чёрча для общерекурсивных функций: любая эффективно-вычислимая функция $\mathbb{N}_0^k \to \mathbb{N}_0$ является общерекурсивной.

def: Запись вида $\psi(\theta_1, \ldots, \theta_n)$ означает $\psi[x_1 := \theta_1, \ldots, x_n := \theta_n]$

def:Литерал числа

$$\overline{a} = \begin{cases} 0, & \text{если } a = 0 \\ (\overline{b})', & \text{если } a = b + 1 \end{cases}$$

Пример: пусть $\psi := x_1 = 0$. Тогда $\psi(\overline{3})$ соответствует формуле $0''' = 0$

4.6 Выразимость отношений в Ф.А.

def: Будем говорить, что отношение $R \subseteq \mathbb{N}_0^n$ **выразимо в ФА**, если существует формула ρ, что:

1. если $\langle a_1, \ldots, a_n \rangle \in R$, то $\vdash \rho(\overline{a_1}, \ldots, \overline{a_n})$
2. если $\langle a_1, \ldots, a_n \rangle \notin R$, то $\vdash \neg\rho(\overline{a_1}, \ldots, \overline{a_n})$

Теорема

Отношение «равно» выразимо в Ф.А.: $R = \{\langle x, x \rangle \mid x \in \mathbb{N}_0\}$

Доказательство:

Пусть $\rho := x_1 = x_2$. Тогда:

- $\vdash p = p$ при $p := \overline{k}$ при всех $k \in \mathbb{N}_0$: $\vdash 0 = 0$, $\vdash 0' = 0'$, $\vdash 0'' = 0''$, ...
- $\vdash \neg p = q$ при $p := \overline{k}$, $q := \overline{s}$ при всех $k, s \in \mathbb{N}_0$ и $k \neq s$.

  $\vdash \neg 0 = 0'$, $\vdash \neg 0 = 0''$, $\vdash \neg 0''' = 0'$, ...

Q.E.D.

4.7 Представимость функций в Ф.А.

def: Будем говорить, что функция $f : \mathbb{N}_0^n \to \mathbb{N}_0$ представима в ФА, если существует формула φ, что:

1. если $f(a_1, \ldots, a_n) = u$, то $\vdash \varphi(\overline{a_1}, \ldots, \overline{a_n}, \overline{u})$
2. если $f(a_1, \ldots, a_n) \neq u$, то $\vdash \neg\varphi(\overline{a_1}, \ldots, \overline{a_n}, \overline{u})$
3. для всех $a_i \in \mathbb{N}_0$ выполнено $\vdash (\exists x.\varphi(\overline{a_1}, \ldots, \overline{a_n}, x))\&(\forall p.\forall q.\varphi(\overline{a_1}, \ldots, \overline{a_n}, p)\&\varphi(\overline{a_1}, \ldots, \overline{a_n}, q) \to p = q)$

4.8 Соответствие рекурсивных и представимых функций

Теорема. Любая рекурсивная функция представима в Ф.А.

Теорема. Любая представимая в Ф.А. функция рекурсивна.

Теорема. Примитивы Z, N и U_n^k представимы в Ф.А.

Доказательство:

- $\zeta(x_1, x_2) := x_2 = 0$, формальнее: $\zeta(x_1, x_2) := x_1 = x_1 \,\&\, x_2 = 0$
- $\nu(x_1, x_2) := x_2 = x_1'$
- $\upsilon(x_1, \ldots, x_n, x_{n+1}) := x_k = x_{n+1}$

  формальнее: $\upsilon(x_1, \ldots, x_n, x_{n+1}) := (\mathop{\&}\limits_{i \neq k, n+1} x_i = x_i) \,\&\, x_k = x_{n+1}$

4.9 Примитив S представим в Ф.А.

$$S\langle f, g_1, \ldots, g_k\rangle(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n))$$

Теорема.

Пусть функции $f, g_1, \ldots, g_k$ представимы в Ф.А. Тогда $S\langle f, g_1, \ldots, g_k\rangle$ представима в Ф.А.

Доказательство:

Пусть f, g_1, ..., g_k представляются формулами φ, γ_1, ..., γ_k.

Тогда $S\langle f, g_1, \ldots, g_k\rangle$ будет представлена формулой

$$\exists g_1. \ldots .\exists g_k.\varphi(g_1, \ldots, g_k, x_{n+1}) \,\&\, \gamma_1(x_1, \ldots, x_n, g_1) \,\&\, \cdots \,\&\, \gamma_k(x_1, \ldots, x_n, g_k)$$

4.10 β-функция Гёделя

Задача: закодировать последовательность натуральных чисел произвольной длины.

def: β-функция Гёделя: $\beta(b, c, i) := b\%(1 + (i + 1) \cdot c)$
Здесь (%) — остаток от деления.

Теорема β-функция Гёделя представима в Ф.А. формулой

$$\hat{\beta}(b, c, i, d) := \exists q.(b = q \cdot (1 + c \cdot (i + 1)) + d)\&(d < 1 + c \cdot (i + 1))$$

Деление b на x с остатком: найдутся частное (q) и остаток (d), что $b = q \cdot x + d$ и $0 \leq d < x$.

Теорема Если $a_0, \ldots, a_n \in \mathbb{N}_0$, то найдутся такие $b, c \in \mathbb{N}_0$, что $a_i = \beta(b, c, i)$

Теорема: Китайская теорема об остатках (вариант формулировки): если $u_0, \ldots, u_n$ — попарно взаимно просты, и $0 \leq a_i < u_i$, то существует такой b, что $a_i = b\%u_i$.

Доказательство:

Положим $c = \max(a_0, \ldots, a_n, n)!$ и $u_i = 1 + c \cdot (i + 1)$.

- НОД$(u_i, u_j) = 1$, если $i \neq j$.

  Пусть p — простое, $u_i \vdots p$ и $u_j \vdots p$ $(i < j)$. Заметим, что $u_j - u_i = c \cdot (j - i)$. Значит, $c \vdots p$ или $(j - i) \vdots p$. Так как $j - i \leq n$, то $c \vdots (j - i)$, потому если и $(j - i) \vdots p$, всё равно $c \vdots p$. Но и $(1 + c \cdot (i + 1)) \vdots p$, отсюда $1 \vdots p$ — что невозможно.

- $0 \leq a_i < u_i$.

Условия китайской теоремы об остатках выполнены и найдётся b, что

$$a_i = b\%(1 + c \cdot (i + 1)) = \beta(b, c, i)$$

Q.E.D.

4.11 Примитив «примитивная рекурсия» представим в Ф.А.

Пусть $f : \mathbb{N}_0^n \to \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$ представлены формулами φ и γ.

Зафиксируем $x_1, \dots, x_n, y \in \mathbb{N}_0$.

Шаг вычисления	Об.	Утверждение в Ф.А.
$R\langle f, g\rangle(x_1, \dots, x_n, 0) = f(x_1, \dots, x_n)$	a_0	$\vdash \varphi(\overline{x_1}, \dots, \overline{x_n}, \overline{a_0})$
$R\langle f, g\rangle(x_1, \dots, x_n, 1) = g(x_1, \dots, x_n, 0, a_0)$	a_1	$\vdash \gamma(\overline{x_1}, \dots, \overline{x_n}, 0, \overline{a_0}, \overline{a_1})$
$\dots$		
$R\langle f, g\rangle(x_1, \dots, x_n, y) = g(x_1, \dots, x_n, y-1, a_{y-1})$	a_y	$\vdash \gamma(\overline{x_1}, \dots, \overline{x_n}, \overline{y-1}, \overline{a_{y-1}}, \overline{a_y})$

По свойству β-функции, найдутся b и c, что $\beta(b, c, i) = a_i$ для $0 \le i \le y$.

Теорема.

Примитив $R\langle f, g\rangle$ представим в Ф.А. формулой $\rho(x_1, \dots, x_n, y, a)$:

$$\begin{aligned}
&\exists b.\exists c.(\exists a_0.\hat{\beta}(b, c, 0, a_0)\&\varphi(x_1, ...x_n, a_0)) \\
\& \quad &\forall k.k < y \to \exists d.\exists e.\hat{\beta}(b, c, k, d)\&\hat{\beta}(b, c, k', e)\&\gamma(x_1, ..x_n, k, d, e) \\
\& \quad &\hat{\beta}(b, c, y, a)
\end{aligned}$$

4.12 Представимость рекурсивных функций в Ф.А.

Теорема.

Пусть функция $f : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$ представима в Ф.А. формулой $\varphi(x_1, \dots, x_n, y, r)$. Тогда примитив $M\langle f\rangle$ представим в Ф.А. формулой

$$\mu(x_1, \dots, x_n, y) := \varphi(x_1, \dots, x_n, y, 0) \,\&\, \forall u.u < y \to \neg\varphi(x_1, \dots, x_n, u, 0)$$

Теорема.

Если f — рекурсивная функция, то она представима в Ф.А.

Индукция по структуре f.

4.13 Рекурсивность представимых в Ф.А. функций

Фиксируем f и $x_1, x_2, \dots, x_n$. Обозначим $y = f(x_1, x_2, \dots, x_n)$. По представимости нам известна φ, что $\vdash \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$. Давайте просто переберём все результаты и доказательства!

1. Закодируем доказательства натуральными числами.
2. Напишем рекурсивную функцию, проверяющую доказательства на корректность.
3. Параллельный перебор значений и доказательств: $s = 2^y \cdot 3^p$. Переберём все s, по s получим y и p. Проверим, что p — код доказательства $\vdash \varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$.

4.14 Гёделева нумерация

1. Отдельный символ.

Номер	Символ	Номер	Символ	Имя	k, n	Гёделев номер
3	(	17	&	0	$0, 0$	$27 + 6$
5	)	19	$\forall$	$(')$	$0, 1$	$27 + 6 \cdot 3$
7	,	21	$\exists$	$(+)$	$0, 2$	$27 + 6 \cdot 9$
9	.	23	$\vdash$	$(\cdot)$	$1, 2$	$27 + 6 \cdot 2 \cdot 9$
11	$\neg$	$25 + 6 \cdot k$	x_k	$(=)$	$0, 2$	$29 + 6 \cdot 9$
13	$\rightarrow$	$27 + 6 \cdot 2^k \cdot 3^n$	f_k^n			
15	$\vee$	$29 + 6 \cdot 2^k \cdot 3^n$	P_k^n			

2. Формула. $\phi \equiv s_0 s_1 \dots s_{n-1}$. Гёделев номер: $\ulcorner\phi\urcorner = 2^{\ulcorner s_0 \urcorner} \cdot 3^{\ulcorner s_1 \urcorner} \cdot \dots \cdot p_{n-1}^{\ulcorner s_{n-1} \urcorner}$.

3. Доказательство. $\Pi = \delta_0 \delta_1 \dots \delta_{k-1}$, его гёделев номер: $\ulcorner\Pi\urcorner = 2^{\ulcorner \delta_0 \urcorner} \cdot 3^{\ulcorner \delta_1 \urcorner} \cdot \dots \cdot p_{k-1}^{\ulcorner \delta_{k-1} \urcorner}$

Теорема.

Следующая функция рекурсивна:

$$\text{proof}(f, x_1, x_2, \dots, x_n, y, p) = \begin{cases} 1, & \text{если} \vdash \phi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y}), \\ & p \text{ — гёделев номер вывода}, f = \ulcorner\phi\urcorner \\ 0, & \text{иначе} \end{cases}$$

Идея доказательства

1. Проверка доказательства вычислима.
2. Согласно тезису Чёрча, любая вычислимая функция вычислима с помощью рекурсивных функций.

Перебор доказательств

Лемма.

Следующие функции рекурсивны:

1. Функции $\text{plog}_k(n) = \max\{p : n : k^p\}$, $\text{fst}(x) = \text{plog}_2(x)$ и $\text{snd}(x) = \text{plog}_3(x)$.
2. Числовые литералы: $\overline{k} : \mathbb{N}_0 \to \mathbb{N}_0$, $\overline{k}(x) = k$.

Теорема.

Если $f : \mathbb{N}_0^n \to \mathbb{N}_0$, и f представима в Ф.А. формулой φ, то f — рекурсивна.

Доказательство:

Пусть заданы $x_1, x_2, \dots, x_n$. Ищем $\langle y, p \rangle$, что $\text{proof}(\ulcorner\varphi\urcorner, x_1, x_2, \dots, x_n, y, p) = 1$, напомним: $y = f(x_1, x_2, \dots, x_n)$, $p = \ulcorner\Pi\urcorner$, Π — доказательство $\varphi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_n}, \overline{y})$.

$$f = S\langle \text{fst}, M\langle S\langle \text{proof}, \overline{\ulcorner\varphi\urcorner}, U_{n+1}^1, U_{n+1}^2, \dots, U_{n+1}^n, S\langle \text{fst}, U_{n+1}^{n+1}\rangle, S\langle \text{snd}, U_{n+1}^{n+1}\rangle\rangle\rangle\rangle$$

5 Лекция 8.

	К.И.В.	И.И.В.	К.И.П.	Ф.А. + кл. модель
корректность	да	да	да	да
непротиворечивость	да	да	да	верим (т. Гёделя №2)
полнота	да	да	да	нет (т. Гёделя №1)
разрешимость	да	да	нет	нет (док-во т. Тарского)

5.1 Классическая модель Ф.А.

А как определять «нестандартные» предикаты и функции (Q_1', $c(p, q)$ и т.п.)? Для простоты разрешим только нелогические функциональные и предикатные символы ($=$, $+$, $\cdot$, 0, $'$).

def: Классическая модель формальной арифметики: $D = \mathbb{N}_0$, оценки предикатных и функциональных символов — естественные.

Теорема.

Формальная арифметика корректна

5.2 Самоприменимость

def: Пусть ξ — формула с единственной свободной переменной x_1. Тогда: $\langle \ulcorner \xi \urcorner, p \rangle \in W_1$, если $\vdash \xi(\overline{\ulcorner \xi \urcorner})$ и p — номер доказательства.

def: Отношение W_1 рекурсивно, поэтому выражено в Ф.А. формулой ω_1 со свободными переменными x_1 и x_2, причём:

1. $\vdash \omega_1(\overline{\ulcorner \varphi \urcorner}, \overline{p})$, если p — гёделев номер доказательства самоприменения φ;
2. $\vdash \neg\omega_1(\overline{\ulcorner \varphi \urcorner}, \overline{p})$ иначе.

Определим формулу $\sigma(x_1) := \forall p.\neg\omega_1(x_1, p)$.

def:Если для любой формулы $\phi(x)$ из $\vdash \phi(0)$, $\vdash \phi(\overline{1})$, $\vdash \phi(\overline{2})$, $\ldots$ выполнено $\nvdash \exists x.\neg\phi(x)$, то теория *омега-непротиворечива.*

Первая теорема Гёделя о неполноте арифметики

- Если формальная арифметика непротиворечива, то $\nvdash \sigma(\overline{\ulcorner \sigma \urcorner})$.
- Если формальная арифметика ω-непротиворечива, то $\nvdash \neg\sigma(\overline{\ulcorner \sigma \urcorner})$.

Доказательство:

Напомним: $\sigma(x_1) := \forall p.\neg\omega_1(x_1, p)$. $W_1(\ulcorner \xi \urcorner, p)$ — p есть доказательство самоприменения ξ.

- Пусть $\vdash \sigma(\overline{\ulcorner \sigma \urcorner})$. Значит, p — номер доказательства. Тогда $\langle \ulcorner \sigma \urcorner, p \rangle \in W_1$. Тогда $\vdash \omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{p})$. Тогда $\vdash \exists p.\omega_1(\overline{\ulcorner \sigma \urcorner}, p)$. То есть $\vdash \neg\forall p.\neg\omega_1(\overline{\ulcorner \sigma \urcorner}, p)$. То есть $\vdash \neg\sigma(\overline{\ulcorner \sigma \urcorner})$. Противоречие.
- Пусть $\vdash \neg\sigma(\overline{\ulcorner \sigma \urcorner})$. То есть $\vdash \exists p.\omega_1(\overline{\ulcorner \sigma \urcorner}, p)$.
  - Но найдётся ли натуральное число p, что $\vdash \omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{p})$? Пусть нет. То есть $\vdash \neg\omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{0})$, $\vdash \neg\omega_1(\overline{\ulcorner \sigma \urcorner}, \overline{1})$, $\ldots$ По ω-непротиворечивости $\nvdash \exists p.\neg\neg\omega_1(\overline{\ulcorner \sigma \urcorner}, p)$.

Значит, найдётся натуральное p, что $\vdash \omega_1(\overline{\ulcorner\sigma\urcorner}, \overline{p})$. То есть, $\langle\ulcorner\sigma\urcorner, p\rangle \in W_1$. То есть, p — доказательство самоприменения σ: $\vdash \sigma(\overline{\ulcorner\sigma\urcorner})$. Противоречие.

Q.E.D.

Почему теорема о неполноте?

def: *Семантически* полная теория — теория, в которой любая общезначимая формула доказуема.

def: *Синтаксически* полная теория — теория, в которой для каждой формулы α выполнено $\vdash \alpha$ или $\vdash \neg\alpha$.

Теорема. Формальная арифметика с классической моделью семантически неполна.

Доказательство:

Рассмотрим Ф.А. с классической моделью. Из теоремы Гёделя имеем $\nvdash \sigma(\overline{\ulcorner\sigma\urcorner})$. Рассмотрим $\sigma(\overline{\ulcorner\sigma\urcorner}) \equiv \forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$: нет числа p, что p — номер доказательства $\sigma(\overline{\ulcorner\sigma\urcorner})$. То есть, $[\![\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)]\!] =$ И. То есть, $\models \sigma(\overline{\ulcorner\sigma\urcorner})$.

Q.E.D.

$\theta_1 \leq \theta_2 \equiv (\exists p.p + \theta_1 = \theta_2) \qquad \theta_1 < \theta_2 \equiv \theta_1 \leq \theta_2 \;\&\; \neg\theta_1 = \theta_2$

Пусть $\langle\ulcorner\xi\urcorner, p\rangle \in W_2$, если $\vdash \neg\xi(\overline{\ulcorner\xi\urcorner})$ и p — номер доказательства. Пусть ω_2 выражает W_2 в формальной арифметике.

Теорема

Рассмотрим $\rho(x_1) = \forall p.\omega_1(x_1, p) \to \exists q.q \leq p \;\&\; \omega_2(x_1, q)$. Тогда $\nvdash \rho(\overline{\ulcorner\rho\urcorner})$ и $\nvdash \neg\rho(\overline{\ulcorner\rho\urcorner})$. $\rho(\overline{\ulcorner\rho\urcorner})$: «Меня легче опровергнуть, чем доказать»

Лемма.

$\vdash 1 = 0$ тогда и только тогда, когда $\vdash \alpha$ при любом α.

def: Обозначим за $\psi(x, p)$ формулу, выражающую в формальной арифметике рекурсивное отношение Proof: $\langle\ulcorner\xi\urcorner, p\rangle \in \text{Proof}$, если p — гёделев номер доказательства ξ.
Обозначим $\pi(x) \equiv \exists p.\psi(x, p)$

def:Формулой Consis назовём формулу $\neg\pi(\overline{\ulcorner 1 = 0\urcorner})$

Неформальный смысл: «формальная арифметика непротиворечива»

5.3 Вторая теорема Гёделя о неполноте арифметики

Теорема. Если Consis доказуем, то формальная арифметика противоречива.

Доказательство:

Формулировка 1 теоремы Гёделя о неполноте арифметики: «если Ф.А. непротиворечива, то недоказуемо $\sigma(\overline{\ulcorner\sigma\urcorner})$». То есть, $\forall p.\neg\omega_1(\overline{\ulcorner\sigma\urcorner}, p)$. То есть, если Consis, то $\sigma(\overline{\ulcorner\sigma\urcorner})$. То есть, если Consis, то $\sigma(\overline{\ulcorner\sigma\urcorner})$, — и это можно доказать, то есть $\vdash \text{Consis} \to \sigma(\overline{\ulcorner\sigma\urcorner})$. Однако если формальная арифметика непротиворечива, то $\nvdash \sigma(\overline{\ulcorner\sigma\urcorner})$.

Рассмотрим такой особый Consis$'$:

$$\begin{aligned}&\pi'(x) := \exists p.\psi(x,p)\ \&\ \neg\psi(\overline{\ulcorner 1=0 \urcorner}, p)\\&\text{Consis}' := \neg\pi'(\overline{\ulcorner 1=0 \urcorner})\end{aligned}$$

Заметим:

1. Если ФА непротиворечива, то $[\![\pi'(x)]\!] = [\![\pi(x)]\!]$:
   - если $x \neq \ulcorner 1=0 \urcorner$ и $[\![\psi(x,p)]\!] = \text{И}$, то $[\![\psi(\overline{\ulcorner 1=0 \urcorner}, p)]\!] = \text{Л}$
   - если $x = \ulcorner 1=0 \urcorner$, то $\psi(\overline{\ulcorner 1=0 \urcorner}, p) = \text{Л}$ при любом p.
2. Но $\vdash \text{Consis}'$.

Q.E.D.

5.4 Условия выводимости Гильберта-Бернайса-Лёба

def: Будем говорить, что формула ψ, выражающая отношение Proof, формула π и формула Consis соответствуют условиям Гильберта-Бернайса-Лёба, если следующие условия выполнены для любой формулы α:

1. $\vdash \alpha$ влечет $\vdash \pi(\overline{\ulcorner \alpha \urcorner})$
2. $\vdash \pi(\overline{\ulcorner \alpha \urcorner}) \to \pi(\overline{\ulcorner \pi(\overline{\ulcorner \alpha \urcorner}) \urcorner})$
3. $\vdash \pi(\overline{\ulcorner \alpha \to \beta \urcorner}) \to \pi(\overline{\ulcorner \alpha \urcorner}) \to \pi(\overline{\ulcorner \beta \urcorner})$

5.5 Первая теорема Гёделя о неполноте ещё раз

Лемма об автоссылках.

Для любой формулы $\phi(x_1)$ можно построить такую замкнутую формулу α (не использующую неаксиоматических предикатных и функциональных символов), что $\vdash \phi(\overline{\ulcorner \alpha \urcorner}) \leftrightarrow \alpha$.

Теорема.

Существует такая замкнутая формула γ, что если Ф.А. непротиворечива, то $\not\vdash \gamma$, а если Ф.А. ω-непротиворечива, то и $\not\vdash \neg\gamma$.

Доказательство:

Рассмотрим $\phi(x_1) \equiv \neg\pi(x_1)$. Тогда по лемме об автоссылках существует γ, что $\vdash \gamma \leftrightarrow \neg\pi(\overline{\ulcorner \gamma \urcorner})$.

- Предположим, что $\vdash \gamma$. Тогда $\vdash \gamma \to \neg\pi(\overline{\ulcorner \gamma \urcorner})$, то есть $\not\vdash \gamma$
- Предположим, что $\vdash \neg\gamma$. Тогда $\vdash \pi(\overline{\ulcorner \gamma \urcorner})$, то есть $\vdash \exists p.\psi(\overline{\ulcorner \gamma \urcorner}, p)$. Тогда по ω-непротиворечивости найдётся p, что $\vdash \psi(\overline{\ulcorner \gamma \urcorner}, \overline{p})$, то есть $\vdash \gamma$.

Q.E.D.

5.6 Доказательство второй теоремы Гёделя

1. Пусть γ таково, что $\vdash \gamma \leftrightarrow \neg\pi(\overline{\ulcorner\gamma\urcorner})$.
2. Покажем $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner 1 = 0 \urcorner})$.
   (a) По условию 2, $\vdash \pi(\overline{\ulcorner\gamma\urcorner}) \to \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner})$. По теореме о дедукции $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner})$;
   (b) Так как $\vdash \pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma$, то по условию 1 $\vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma\urcorner})$;
   (c) По условию 3, $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner}) \to \neg\gamma\urcorner}) \to \pi(\overline{\ulcorner\pi(\overline{\ulcorner\gamma\urcorner})\urcorner}) \to \pi(\overline{\ulcorner\neg\gamma\urcorner})$;
   (d) Таким образом, $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner\neg\gamma\urcorner})$;
   (e) Однако $\vdash \gamma \to \neg\gamma \to 1 = 0$. Условие 3 (применить два раза) даст $\pi(\overline{\ulcorner\gamma\urcorner}) \vdash \pi(\overline{\ulcorner 1 = 0\urcorner})$.
3. $\vdash \neg\pi(\overline{\ulcorner 1 = 0\urcorner}) \to \neg\pi(\overline{\ulcorner\gamma\urcorner})$ (т. о дедукции, контрапозиция).
4. $\vdash \neg\pi(\overline{\ulcorner 1 = 0\urcorner}) \to \gamma$ (определение γ).

5.7 Расширение на другие теории

def: Теория $\mathcal{S}$ — расширение теории $\mathcal{T}$, если из $\vdash_{\mathcal{T}} \alpha$ следует $\vdash_{\mathcal{S}} \alpha$

def: Теория $\mathcal{S}$ — рекурсивно-аксиоматизируемая, если найдётся теория $\mathcal{S}'$ с тем же языком, что:

1. $\vdash_{\mathcal{S}} \alpha$ тогда и только тогда, когда $\vdash_{\mathcal{S}'} \alpha$;
2. Множество аксиом теории $\mathcal{S}'$ рекурсивно.

Теорема.

Если $\mathcal{S}$ — непротиворечивое рекурсивно-аксиоматизируемое расширение формальной арифметики, то в ней можно доказать аналоги теорем Гёделя о неполноте арифметики.

5.8 Сужение: система Робинсона

def: Теория первого порядка, использующая нелогические функциональные символы 0, $(+)$ и $(\cdot)$, нелогический предикатный символ $(=)$ и следующие нелогические аксиомы, называется системой Робинсона.

$$\begin{array}{ll}
a = a & a = b \to b = a \\
a = b \to b = c \to a = c & a = b \to a' = b' \\
a' = b' \to a = b & \neg 0 = a' \\
a = b \to a + c = b + c \,\&\, c + a = c + b & a = b \to a \cdot c = b \cdot c \,\&\, c \cdot a = c \cdot b \\
\neg a = 0 \to \exists b. a = b' & a + 0 = a \\
a + b' = (a + b)' & a \cdot 0 = 0 \\
a \cdot b' = a \cdot b + a &
\end{array}$$

Система Робинсона неполна: аксиомы — в точности утверждения, необходимые для доказательства теорем Гёделя. Система Робинсона не имеет схем аксиом.

5.9 Арифметика Пресбургера

def: Теория первого порядка, использующая нелогические функциональные символы 0, 1, (+), нелогический предикатный символ (=) и следующие нелогические аксиомы, называется арифметикой Пресбургера.

$$\begin{aligned}
&\neg(0 = x + 1)\\
&x + 1 = y + 1 \to x = y\\
&x + 0 = x\\
&x + (y + 1) = (x + y) + 1\\
&(\varphi(0) \,\&\, \forall x.\varphi(x) \to \varphi(x + 1)) \to \forall y.\varphi(y)
\end{aligned}$$

Теорема. Арифметика Пресбургера разрешима и синтаксически и семантически полна.

5.10 Невыразимость доказуемости

$\mathrm{Th}_{\mathcal{S}} = \{\ulcorner\alpha\urcorner \mid \vdash_{\mathcal{S}} \alpha\}$; $\mathrm{Tr}_{\mathcal{S}} = \{\ulcorner\alpha\urcorner \mid [\![\alpha]\!]_{\mathcal{S}} = \text{И}\}$

Лемма.

Пусть $D(\ulcorner\alpha\urcorner) = \ulcorner\alpha(\overline{\ulcorner\alpha\urcorner})\urcorner$ для любой формулы $\alpha(x)$. Тогда D представима в формальной арифметике.

Теорема. Если расширение Ф.А. $\mathcal{S}$ непротиворечиво и D представима в нём, то $\mathrm{Th}_{\mathcal{S}}$ невыразимо в $\mathcal{S}$

Даказательство:

Пусть $\delta(a, p)$ представляет D, и пусть $\sigma(x)$ выражает множество $\mathrm{Th}_{\mathcal{S}}$ (рассматриваемое как одноместное отношение).

Пусть $\alpha(x) := \forall p.\delta(x, p) \to \neg\sigma(p)$. Верно ли, что $\ulcorner\alpha\urcorner \in \mathrm{Th}_{\mathcal{S}}$?

Q.E.D.

5.11 Неразрешимость формальной арифметики

Теорема.

Если формальная арифметика непротиворечива, то формальная арифметика неразрешима

Доказательство:

Пусть формальная арифметика разрешима. Значит, есть рекурсивная функция $f(x)$: $f(x) = 1$ тогда и только тогда, когда $x \in \mathrm{Th}_{\text{Ф.А.}}$. То есть, $\mathrm{Th}_{\text{Ф.А.}}$ выразимо в формальной арифметике.

По теореме о невыразимости доказуемости, $\mathrm{Th}_{\text{Ф.А.}}$ невыразимо в формальной арифметике. Противоречие.

Q.E.D.

Теорема Тарского о невыразимости истины Не существует формулы $\varphi(x)$, что $[\![\varphi(\overline{x})]\!] = \text{И}$ (в стандартной интерпретации) тогда и только тогда, когда $x \in \mathrm{Tr}_{\text{ФА}}$.

Доказательство:

Пусть теория $\mathcal{S}$ — формальная арифметика + аксиомы: все истинные в стандартной интерпретации формулы. Очевидно, что $\mathrm{Th}_{\mathcal{S}} = \mathrm{Tr}_{\mathcal{S}} = \mathrm{Tr}_{\Phi\mathrm{A}}$. То есть $\mathrm{Tr}_{\Phi\mathrm{A}}$ невыразимо в $\mathcal{S}$.

Пусть φ таково, что $[\![\varphi(\overline{x})]\!] =$ И при $x \in \mathrm{Tr}$. Тогда $\vdash \varphi(\overline{x})$, если $x \in \mathrm{Tr}$ и $\vdash \neg\varphi(\overline{x})$, если $x \notin \mathrm{Tr}$.

Тогда Tr выразимо в $\mathcal{S}$. Противоречие.

Q.E.D.

Однако, если взять $D = \mathbb{R}$, истина становится выразима (алгоритм Тарского).

6 Информация о курсе.

Поток — y2024.
Группы M3132-M3139.
Преподаватель — Штукенберг Дмитрий Григорьевич.

Нам пизда, ребятки.